

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN**

DANA MANZA, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

PESI, INC.,

Defendant.

Case No.: 3:24-cv-000690-amb

DEMAND FOR JURY TRIAL

AMENDED CLASS ACTION COMPLAINT

INTRODUCTION

Dana Manza (“Plaintiff”), individually and on behalf of all others similarly situated, makes the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to herself or her counsel, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiff brings this action to redress Defendant PESI, Inc.’s (“PESI”) practice of selling, renting, transmitting, and/or otherwise disclosing, to various third parties, records containing the personal information (including names and addresses) of each of their customers, along with detailed information revealing the titles and subject matter of the videos and other audiovisual materials purchased by each customer (collectively “Personal Viewing Information”) in violation of the Video Privacy Protection Act, 18 U.S.C. § 2710 et seq. (“VPPA”).

2. Defendant violated the VPPA with respect to its disclosure of Plaintiff’s and Class members’ Personal Viewing Information in two ways.

3. First, Defendant disclosed its customers’ Personal Viewing Information to various third-party recipients, which then appended that information to a myriad of other categories of personal and demographic data pertaining to those customers. Defendant re-sells that Personal Viewing Information (with the appended demographic information) to other third parties on the open market.

4. Second, Defendant systematically transmitted (and continues to transmit today) its customers' personally identifying video purchase information to third parties, such as Meta Platforms, Inc. ("Meta"), Alphabet, Inc. f/k/a Google ("Google"), and Pinterest, Inc. ("Pinterest") using snippets of programming code (collectively, "Tracking Technologies"). The programming code for Meta is called the "Meta Pixel," which Defendant chose to install on its www.pesi.com website (the "Website"). Defendant's website uses "Google Analytics" technology and the programming code for that technology is the "Google Tag Manager,"¹ which Defendant chose to integrate and install on its website (hereinafter, "Google Analytics"). The programming code for Pinterest is called the "Pinterest Tag," which Defendant chose to install on its website.

5. The information Defendant disclosed (and continues to disclose) to Meta via the Meta Pixel includes the customer's Facebook ID ("FID") and the subscription that each of its customers purchased on its Website. An FID is a unique sequence of numbers linked to a specific Meta profile. A Meta profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person). Entering "Facebook.com/[FID]" into a web browser returns the Meta profile of the person to

¹ Google Developers, About Google Tag Manager, <https://developers.google.com/tag-platform/tag-manager> (last visited Oct. 2, 2024).

whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name, but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta information that reveals a particular person purchased prerecorded video to access prerecorded video content from Defendant's Website, information which is hereinafter, referred to as "Personal Viewing Information."

6. Similarly, Google Analytics and the Pinterest Tag were intentionally installed by Defendant on its Website. The information Defendant disclosed (and continues to disclose) to Google Analytics via the Google Tag Manager it installed on its website includes the specific video title and unique user data sufficient for identification of the subscriber.

7. The information Defendant disclosed (and continues to disclose) to Pinterest via the Pinterest Tag it installed on its website includes the specific video title alongside Pinterest account holder's "user id" ("uid"), which can be used to identify the particular user.

8. Defendant disclosed, continues to disclose, and allows for the surreptitious collection of its customers' Personal Viewing Information to these third parties without asking for, let alone obtaining, their consent to these practices.

9. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), damages in the amount of \$2,500.00, *see id.* § 2710(c).

10. Thus, while Defendant profits handsomely from their unauthorized disclosures of their customers' Personal Viewing Information to third parties without providing prior notice to or obtaining the requisite consent from any of these customers, they do so at the expense of their customers' privacy and their statutory rights under federal law.

11. Defendant's practice of disclosing its customers' Personal Viewing Information in violation of the VPPA has invaded Plaintiff's and the other unnamed Class members' privacy and resulted in a barrage of unwanted junk mail to their home addresses and e-mail inboxes. Defendant's disclosure is also dangerous because it allows for the targeting of particularly vulnerable members of society. For example, and as a result of Defendant's disclosure of Personal Viewing Information, any person or entity could buy a list with the names and addresses of all women residing in a particular state who have purchased and attended mental health or healthcare nursing

seminars on a specified topic during the past 12 months. Such lists are available for sale for approximately \$155.00 and \$180.00 per thousand customers listed.

12. In an era when the collection and monetization of consumer data proliferate on an unprecedented scale, it is important that companies are held accountable for the exploitation of their customers' sensitive information. Defendant chose to disregard Plaintiff's and thousands of other consumers' statutorily protected privacy rights by (a) releasing their Personal Viewing Information into the data-aggregation and brokerage marketplace and (b) directly disseminating such information from its websites to Meta, Google, and Pinterest via Tracking Technologies. Accordingly, on behalf of herself and the putative Classes defined below, Plaintiff brings this Amended Class Action Complaint against Defendant for intentionally and unlawfully disclosing her and the Classes' Personal Viewing Information.

PARTIES

I. Plaintiff Dana Manza

13. Plaintiff is, and at all times relevant hereto was, a citizen and resident of Nassau County, New York.

14. Plaintiff is, and at all times relevant hereto was, a user of Meta.

15. Plaintiff is a consumer of the video products and services offered on Defendant's www.pesi.com website. Including on or about January 3, 2023, Plaintiff

purchased prerecorded video material from Defendant's website by requesting and paying for such material, providing her name, email address, and home address for delivery of such material. Defendant completed its sales of goods to Plaintiff by delivering the prerecorded video material she purchased to the address she provided in her order. Accordingly, Plaintiff requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its website.

16. At all times relevant hereto, including when purchasing, requesting, and obtaining the prerecorded video material from Defendant's website, Plaintiff had a Meta account, a Meta profile, and an FID associated with such profile.

17. At all times relevant hereto, including when purchasing, requesting, and obtaining the prerecorded video material from Defendant's website, Plaintiff had Google and Pinterest accounts, corresponding profiles, and unique identifiers associated with such profiles.

18. When Plaintiff purchased prerecorded video material from Defendant on its website, Defendant separately disclosed Plaintiff's FID, Plaintiff's Pinterest "uid" directly associated with her Pinterest account, and excessive amounts of device and uniquely identifiable data points about Plaintiff to Google Analytics coupled with the specific title of the prerecorded video or video materials she purchased (as well as the URL where such video is available for purchase), among other information concerning Plaintiff and the device on which she used to make the

purchase (the purchaser’s unique IP address, browser description, device name and type, and geolocation information).

19. To illustrate Defendant’s disclosure to Meta, when Plaintiff purchased the “Integrative Sex and Couples Certification Training with Tammy Nelson: Certified Sex Therapy Informed Professional (CSTIP)” course, the specific title of the prerecorded video, the product code: 001608, and her request to “go to checkout” to complete her purchase was transmitted to Meta alongside Plaintiff’s FID as seen in the exemplar source code below obtained by Counsel below:

▼ General	
Request URL:	https://www.facebook.com/privacy_sandbox/pixel/register/trigger/?id=1605037483099710&ev=SubscribedButtonClick&dl=https%3A%2F%2Fcatalog.pesi.com%2Fshoppingcart&rl=https%3A%2F%2Fcatalog.pesi.com%2Fsales%2Fbh_c_001608_integrativesexcouplescertification_organic-404417_if=false&ts=1727449144780&cd[buttonFeatures]=%7B%22classList%22%3A%22pull-right%20btn%20btn-primary%20ce21_cart_clsProceedToCart%20clsProceedToCart%22%2C%22destination%22%3A%22javascript%3Avoid(0)%3B%22%2C%22id%22%3A%22btnProceedToCheckout%22%2C%22imageUrl%22%3A%22linear-gradient(rgb(51%2C%2012%2C%20183)%200%25%2C%20rgb(38%2C%2090%2C%20136)%20100%25)%22%2C%22innerText%22%3A%22Proceed%20to%20checkout%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonText]=Proceed%20to%20checkout&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Shopping%20Cart%20%7C%20PESI.com%22%7D&sw=3008&sh=1692&v=2.9.168&r=stable&ec=1&o=4126&fbp=fb.1.1726589158520.397865688563904186&ler=other&cdl=API_unavailable&it=1727449139766&coo=false&es=automatic&tm=3&rqm=FGET
Request Method:	GET
Status Code:	● 200 OK
Remote Address:	31.13.67.35:443
Referrer Policy:	strict-origin-when-cross-origin

20. To illustrate Defendant’s disclosure to Google Analytics, when Plaintiff made her purchase, her request or initiation of the purchase, the title of the

prerecorded video content to be purchased, and the prerecorded video content's product number were transmitted to Google Analytics alongside Plaintiff's unique device identifiers (including cid,² uid,³ and NID⁴) as seen in the exemplar source code obtained by Counsel below:

² Google Analytics Help, [GA4] Data collection, <https://support.google.com/analytics/answer/11593727?hl=en> (last visited Sept. 28, 2024) ("Google Analytics stores a client ID in a first-party cookie named _ga to distinguish unique users and their sessions on your website. ").

³ Google Analytics Help, User-ID Feature, <https://support.google.com/analytics/answer/3123662#zippy=%2Cin-this-article> (last visited Sept. 28, 2024) ("User-ID lets you associate a persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices . . . User-ID enables the association of one or more sessions (and the activity within those sessions) with a unique and persistent ID that you send to Analytics. ").

⁴ Google, *How Google uses cookies*, <https://policies.google.com/technologies/cookies> (last visited Sept. 28, 2024) ("The 'NID' cookie is used to show Google ads in Google services for *signed-out users*") (emphasis added).

▼ Request Headers

```

:authority:          www.google.com
:method:            GET
:path:              /pagead/1p-user-list/877718457/?
                    random=1727454316557&cv=11&fst=1727452800000&bg=ffffff&
                    guid=ON&async=1&gtm=45je49p0v872775561z872104490za20
                    0zb72104490&gcd=13l3l3l3l1l1&dma=0&tag_exp=101671035~10
                    1747727&u_w=3008&u_h=1692&url=https%3A%2F%2Fcatalog.p
                    esi.com%2Fshoppingcart&ref=https%3A%2F%2Fcatalog.pesi.co
                    m%2Fsales%2Fbh_c001608_integrativesexcouplescertification
                    organic-
                    404417&hn=www.googleadservices.com&frm=0&tiba=Shopping
                    %20Cart%20%7C%20PESI.com&npa=0&pscdl=noapi&auid=2069
                    447533.1726589158&uaa=arm&uab=64&uafvl=Chromium%3B12
                    8.0.6613.139%7CNot%253BA%253DBrand%3B24.0.0.0%7CGoog
                    le%252CChrome%3B128.0.6613.139&uamb=0&uam=&uap=macO
                    S&uapv=14.5.0&uaw=0&fledge=1&data=event%3Dgtag.config&rft
                    mt=3&fmt=3&is_vtc=1&cid=CAQSKQDpaXnfUGOjPcZLNDRU5wb
                    2f3B7s2peKIOYaTe75iRU85ux1tr94rjc&random=1340292074&rmt
                    _tld=0&ipr=y
:scheme:            https
Accept:             image/avif,image/webp,image/apng,image/svg+xml,image/*/*;q=
                    0.8
Accept-Encoding:    gzip, deflate, br, zstd
Accept-Language:    en-US,en;q=0.9
Cookie:             __Secure-
                    3PSID=g.a000oAijefLf5vQwittvnZvr69Q05ruzIMtAP6LZt_79Mvwg
                    xGCuYXL25vpYY_AsTvKh1TlgJgACgYKAQ4SARESFQHGX2MiCY9
                    emM202jqeinlz-
                    oflqRoVAUF8yKrV6bnH5uKOGFvymK_cYnBG0076; __Secure-
                    3PAPISID=kxJ-Z8bQoZxQCxdP/APnz71wo2CfQSS_F8;
                    NID=517=v_wdHz3adxRYvj621yF2-
                    GpP31JOs6h6IMnvrlBSbb7j37GgUEc6fkOSEh1SbPevdhgWYM08
                    w7HMhuJQPOodvIrprJQwSCedxl_dHriF7rLlp4LSKbsoU5rJQo11B9
                    N5rtV96pSqnaO0063gdzP3DytkU5WM5d7MGY1gfUYoudwMgM

```

21. The same information within the request headers seen above that was sent to Google Analytics was sent to “Google Adsense” and “Google Leads” in the source code when Plaintiff made her purchase.

22. To illustrate Defendant’s disclosure to Pinterest, when Plaintiff made her purchase, her request or initiation of the purchase – “add to cart event”, order quantity, the title of the prerecorded video content to be purchased, product category,

and the prerecorded video content's product number and price were transmitted to the Pinterest alongside Plaintiff's unique identifiers (s_a value⁵) as seen in the examples obtained by Counsel below:

⁵ Pinterest uses a "s_a" cookie that contains an encrypted string of letters, numbers, and characters. The s_a cookie identifies users across devices and webpages because the value is the same whether a person is on their Pinterest account or a webpage with the Pinterest Tag enabled.

Request URL: [https://ct.pinterest.com/v3/?event=addtocart&event_id=7B%22product_name%22%3A%22Integrative%20Sex%20and%20Couples%20Certification%20Training%20with%20Tammy%20Nelson%3A%20Certified%20Sex%20Therapy%20Informed%20Professional%20\(CSTIP\)%20Course%22%2C%22product_price%22%3A1319.81%2C%22np%22%3A%22gtm%22%2C%22order_quantity%22%3A1%2C%22value%22%3A725.9%2C%22currency%22%3A%22USD%22%2C%22line_items%22%3A%5B%7B%22product_id%22%3A%22106648%22%2C%22product_category%22%3A%22Online%20Course%22%7D%5D%22%22event_id%22%3A%223b2f4e27-982b-4d06-b784-a66d2f58dc9e%22%7D&tid=2613831277235&pd=%7B%22np%22%3A%22gtm%22%2C%22pin_unauth%22%3A%22dWlKPvPvUSTJaREV4WmpndFpESTNaaTAwWIRGaUxUazVPREV0Wm1SaFI6QTNNRFV5ThpBMA%22%2C%22derived_epik%22%3A%22dj0yJnU9SURaV3ICNHlxdm1XSzgzYlhxSJNDRWRFUVR2LUpSbWwmbj04WWRYsXJCS25wZnk3V1ZoR0stZUtBjM09MSZ0PUFBQUFBR2lyMjZFJnJtPTEmcnQ9QUFBQUFHjYjlyNkUmc3A9NQ%22%2C%22aem_fn%22%3A%22ce375f9c38ced0ab298c9b4360ea4013c911eafce3c98bab9f89f23f98e0f012%22%2C%22aem_eligible_list%22%3A%5B%22fn%22%5D%7D&ad=%7B%22loc%22%3A%22https%3A%2F%2Fcatalog.pesi.com%2Fsales%22%22%22bh_c_001608_integrativesexcouplescertification_organic-404417%22%2C%22ref%22%3A%22https%3A%2F%2Fwww.google.com%2F%22%2C%22if%22%3Afalse%2C%22sh%22%3A1692%2C%22sw%22%3A3008%2C%22mh%22%3A%2297c41ef3%22%2C%22is_eu%22%3Afalse%2C%22epikDataSource%22%3Anull%2C%22derivedEpikDataSource%22%3A%22fpc_ls%22%2C%22unauthldDataSource%22%3A%22fpc_ls%22%2C%22architecture%22%3A%22arm%22%2C%22bitness%22%3A%2264%22%2C%22brands%22%3A%5B%7B%22brand%22%3A%22Chromium%22%2C%22version%22%3A%22128%22%7D%2C%7B%22brand%22%3A%22Not%3BA%3DBrand%22%2C%22version%22%3A%2224%22%7D%2C%7B%22brand%22%3A%22Google%20Chrome%22%2C%22version%22%3A%22128%22%7D%5D%2C%22mobile%22%3Afalse%2C%22model%22%3A%22%22%2C%22platform%22%3A%22macOS%22%2C%22platformVersion%22%3A%2214.5.0%22%2C%22uaFullVersion%22%3A%22128.0.6613.139%22%2C%22ecm_enabled%22%3Atrue%7D&cb=1727454132498&dbgppce=true](https://ct.pinterest.com/v3/?event=addtocart&event_id=7B%22product_name%22%3A%22Integrative%20Sex%20and%20Couples%20Certification%20Training%20with%20Tammy%20Nelson%3A%20Certified%20Sex%20Therapy%20Informed%20Professional%20(CSTIP)%20Course%22%2C%22product_price%22%3A1319.81%2C%22np%22%3A%22gtm%22%2C%22order_quantity%22%3A1%2C%22value%22%3A725.9%2C%22currency%22%3A%22USD%22%2C%22line_items%22%3A%5B%7B%22product_id%22%3A%22106648%22%2C%22product_category%22%3A%22Online%20Course%22%7D%5D%22%22event_id%22%3A%223b2f4e27-982b-4d06-b784-a66d2f58dc9e%22%7D&tid=2613831277235&pd=%7B%22np%22%3A%22gtm%22%2C%22pin_unauth%22%3A%22dWlKPvPvUSTJaREV4WmpndFpESTNaaTAwWIRGaUxUazVPREV0Wm1SaFI6QTNNRFV5ThpBMA%22%2C%22derived_epik%22%3A%22dj0yJnU9SURaV3ICNHlxdm1XSzgzYlhxSJNDRWRFUVR2LUpSbWwmbj04WWRYsXJCS25wZnk3V1ZoR0stZUtBjM09MSZ0PUFBQUFBR2lyMjZFJnJtPTEmcnQ9QUFBQUFHjYjlyNkUmc3A9NQ%22%2C%22aem_fn%22%3A%22ce375f9c38ced0ab298c9b4360ea4013c911eafce3c98bab9f89f23f98e0f012%22%2C%22aem_eligible_list%22%3A%5B%22fn%22%5D%7D&ad=%7B%22loc%22%3A%22https%3A%2F%2Fcatalog.pesi.com%2Fsales%22%22%22bh_c_001608_integrativesexcouplescertification_organic-404417%22%2C%22ref%22%3A%22https%3A%2F%2Fwww.google.com%2F%22%2C%22if%22%3Afalse%2C%22sh%22%3A1692%2C%22sw%22%3A3008%2C%22mh%22%3A%2297c41ef3%22%2C%22is_eu%22%3Afalse%2C%22epikDataSource%22%3Anull%2C%22derivedEpikDataSource%22%3A%22fpc_ls%22%2C%22unauthldDataSource%22%3A%22fpc_ls%22%2C%22architecture%22%3A%22arm%22%2C%22bitness%22%3A%2264%22%2C%22brands%22%3A%5B%7B%22brand%22%3A%22Chromium%22%2C%22version%22%3A%22128%22%7D%2C%7B%22brand%22%3A%22Not%3BA%3DBrand%22%2C%22version%22%3A%2224%22%7D%2C%7B%22brand%22%3A%22Google%20Chrome%22%2C%22version%22%3A%22128%22%7D%5D%2C%22mobile%22%3Afalse%2C%22model%22%3A%22%22%2C%22platform%22%3A%22macOS%22%2C%22platformVersion%22%3A%2214.5.0%22%2C%22uaFullVersion%22%3A%22128.0.6613.139%22%2C%22ecm_enabled%22%3Atrue%7D&cb=1727454132498&dbgppce=true)

Request Method: GET

Status Code: 200 OK

Remote Address: 151.101.192.84:443

Referrer Policy: strict-origin-when-cross-origin

```
s_a=YkNEa3Y4ZmYrOW1xNXI5Z0RTOVVaSFZmV0hYtIZpcVZIY0
1UXlndVVrTExpdGpwQVBarU1oUG4yM2thWFh0RjRvV3RyTWJh
zUxWHpMbXhhY3R0bjhPRmtJdTFTUnlxZTJFSFhSNFpWUmNLV
s3WjBaNUpYS2N0QjI4ZzR3RTISQVF0bGJKZ3NRRUVUaEJTam4
eUtWMWdlY1ZYdHZVc25TWEZqMHVSdDZTTVNuMnExUzdFaEF
HRoZ0FGZHV2cDJpS2ILYTRqbXZXU3FoQTkwYkwwOHJoTUIIVK
OMnM1RGx2SjY0c0IPemZKL3RYVkgymRFKzZwSHowanRGOFZ
RU5oMWorMWkzaVkyQy8wNnlaSFZJZWZSZnY5ZFgza2RYVS9I
UIZoL281ZDNsb29tNWl4MzdKdmJOuUUVzN0N4UEt5MzhMWW1
YIVZbGZRbmtEbkVIK054R0pCN1VGLzJIL090c1RaSU9EMDVYc
wOHlyOVNUOTZadWk5TEJ1djc2KzQrUm1xL3ZDTIZLQzc5OXds
XNVNU5QbER2OGtSQzA5SGtarWpEU09KT1RhMDJnS0UyMHU
zJHQ0puSW5RZ005a0FpVIRrMTBiVDBhZ0VSSnc1MEhVK2NEQ
JUMDV5T2E5WGJCMkd2R2p3SmFmOFc4aXV2bFVXbkYzd2h6e
c4YVgzMmpKcXJXYmVHRTdsZ29PdE1ocUF0eWJDaeXsZlRpeml
SGFQU2pBeS9UbmE3QUJOajh0ajVqL2g0TVcwVTJBRXFvL0RxV
hHVZcvWTNIYjRUVXpJUnlpNDBSQVU4VitqN09ldG1kWTvNcEJl
UUJTR3dEcZJrVTgzVUplV1RZVjgyb0t2Y0I4SUJNQW1aenBBd21
cm55RzZxc002d0c3TnVxcKwRv0FZeE9aZ3JkY3h4ZWNNTEhYK
0rZ1g2YUtPYUp5Yi9Wa2puR3JCUnd1bUN3ay9OOWVGvWJwT1
BOEhRdmN0a1lqS2t6YIUxSitPUW9uaDBJLZdsVXpMOXhmcUx5
UJ2azA4NHA3amw2UENPUjcwN1Z5bGFFZFNwQm9kOTc1ZHV4
EIHYN2TEk9FQ2FzZl1L0xNL1hqdm5mcjVYwJRQKzNlcTE2MGxI
VzZnVU1DdFQvYnFUS0tDbVh1RVgyZWVxek5BSEZ5TUVYmmtjZ
U4cU9Zd2pQRG9jaXE3L1pwT3JwaGxGWjlzMEthcU9qU3ZqY0p
FQ0Skd3VEJZVmxnSkQ4L2lraUkwV21rbTIRcjdVcGgrMUvWQitS
BqNG5xeTJ6cFRqSWhtT1BhekFPZm5NZW8zcWJZT1FZcDhzWT
mZ01YQk9yT2NwVXhhSmErRDVWNjhiS2IzNjV3PQ==;
_pinterest_ct_ua="TWc9PSZUa1BWQWhNdmdvOVFTcng0NjJxa
TOUUrQ2JHMFIXUkdRd21aTENBaUNtb1UvME83TzhKUEZ3YUE
WUvUHFIZDIWWUdDWUI4c1VVSWFcrUFjenc2N3p3dUsranBFZ
RMSjIKVW1YSIhSMD0mSmh1VTJFZ1FGUihzbVlxY3VkU2YwT3ZV
SmRzPQ==";
```

23. Prior to and at the time she purchased prerecorded video material from Defendant, Defendant did not notify Plaintiff that it would disclose the Personal Viewing Information of its customers generally or that of Plaintiff in particular, and Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Personal Viewing Information to third parties. Plaintiff has never been provided any written notice that Defendant sells, rents, licenses, exchanges, or

otherwise discloses its customers' Personal Viewing Information, or any means of opting out of such disclosures of her Personal Viewing Information.

24. Defendant nonetheless sold, rented, transmitted and/or otherwise disclosed, either directly or through an intermediary or intermediaries, Plaintiff's Personal Viewing Information to data miners, data appenders, data aggregators, marketing companies, and/or other third parties, including without limitation NextMark, during the relevant time period.

25. Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Personal Viewing Information to third parties. In fact, Defendant has never even provided Plaintiff with written notice of its practices of disclosing its customers' Personal Viewing Information to third parties.

26. Because Defendant disclosed Plaintiff's Personal Viewing Information (including her FID, unique identifiers, and her purchase of prerecorded video material to Defendant's website) to third parties during the applicable statutory period, Defendant violated Plaintiff's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

II. Defendant PESI, Inc.

27. Defendant is a non-stock corporation existing under the laws of the State of Wisconsin with a principal place of business at 3839 White Ave.,

Eau Claire, WI 54703. Defendant operates and maintains the Website www.pesi.com, where it carries out its mission and most significant activity which is to provide education and training to healthcare professionals, counseling professionals, and the general public through the sale and delivery of prerecorded video content including: conferences, seminars, workshops, online/on-demand courses, CDs and DVDs on various topics.

28. Defendant also utilizes, governs, and maintains a network of affiliates, such as the Psychotherapy Networker and others, to sell its prerecorded video content on their respective websites.⁶

JURISDICTION AND VENUE

29. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

30. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in Eau Claire, WI, within this judicial District.

VIDEO PRIVACY PROTECTION ACT

31. The VPPA prohibits companies (like Defendant) from knowingly disclosing to third parties (like Meta, Google, and Pinterest) information that

⁶ Where “Website” is referenced herein, it refers to www.pesi.com and any of Defendant’s affiliate websites.

personally identifies consumers (like Plaintiff) as having requested or obtained particular videos or other audio-visual materials.

32. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits “a video tape service provider” from “knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]” 18 U.S.C. § 2710(b)(1). The statute defines a “video tape service provider” as “any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials,” 18 U.S.C. § 2710(a)(4). It defines a “consumer” as “a renter, purchaser, or subscriber of goods or services from a video tape service provider.” 18 U.S.C. § 2710(a)(1). “[P]ersonally identifiable information” includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3).

33. Leading up to the VPPA’s enactment in 1988, members of the United States Senate warned that “[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes.” *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers’ purchases and rentals of videos and other audiovisual materials because such records offer “a window into our loves, likes, and dislikes,” such that “the trail of information generated by every

transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance.” S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

34. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that “our right to privacy protects the choice of movies that we watch with our family in our own homes.” 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, the personal nature of such information, and the need to protect it from disclosure, is the *raison d’être* of the statute: “These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people.” *Id.*

35. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a more recent Senate Judiciary Committee meeting, “The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century,” Senator Leahy emphasized the point by stating: “While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the ‘cloud,’

mobile apps and other new technologies have revolutionized the availability of Americans' information.”⁷

36. Former Senator Al Franken may have said it best: “If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn’t. The Video Privacy Protection Act guarantees them that right.”⁸

37. In this case, however, Defendant deprived Plaintiff and numerous other similarly situated persons of that right by systematically (and surreptitiously) disclosing their Personal Viewing Information to third parties, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers’ Personal Information Has Real Market Value

38. In 2001, Federal Trade Commission (“FTC”) Commissioner Orson Swindle remarked that “the digital revolution . . . has given an enormous capacity

⁷ The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, <http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury>.

⁸ Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, franken.senate.gov (Jan. 31, 2012).

to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves.”⁹

39. Over two decades later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a 26 billion dollar per year online advertising industry in the United States.¹⁰

40. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.¹¹

41. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about

⁹ Transcript, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

¹⁰ See Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), available at <https://www.wsj.com/articles/SB10001424052748703529004576160764037920274>.

¹¹ Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

consumers. Data aggregators then profit by selling this “extraordinarily intrusive” information in an open and largely unregulated market.¹²

42. The scope of data aggregators’ knowledge about consumers is immense: “If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on.”¹³

43. Further, “[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available.”¹⁴

44. Recognizing the severe threat the data mining industry poses to consumers’ privacy, on July 25, 2012, the co-chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

¹² See M. White, *Big Data Knows What You’re Doing Right Now*, TIME.com (July 31, 2012), available at <http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/>.

¹³ N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), available at <https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html#:~:text=It's%20called%20the%20Acxiom%20Corporation,to%20know%20much%20C%20much%20more>.

¹⁴ Letter from Sen. J. Rockefeller IV, Sen. Cmtee. On Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) available at <https://www.commerce.senate.gov/services/files/3bb94703-5ac8-4157-a97b-%20a658c3c3061c>.

By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.¹⁵

45. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like PESI share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the “[v]ast databases” of consumer data that are often “sold to thieves by large publicly traded companies,” which “put[s] almost anyone within the reach of fraudulent telemarketers” and other criminals.¹⁶

46. Disclosures like Defendant’s are particularly dangerous to the elderly. “Older Americans are perfect telemarketing customers, analysts say, because they

¹⁵ See *Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers’ Personal Information*, Website of Sen. Markey (July 24, 2012), available at <https://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information>.

¹⁶ See Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at <https://www.nytimes.com/2007/05/20/business/20tele.html>.

are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide.”¹⁷

47. The FTC notes that “[t]he elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers.”¹⁸

48. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like Defendant’s are particularly troublesome because of their cascading nature: “Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists.”¹⁹

49. Defendant is not alone in violating its customers’ statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

¹⁷ *Id.*

¹⁸ Prepared Statement of the FTC on “Fraud Against Seniors” before the Special Committee on Aging, United States Senate (August 10, 2000).

¹⁹ *Id.*

II. Consumers Place Monetary Value on Their Privacy and Consider Privacy Practices When Making Purchases

50. As the data aggregation industry has grown, so has consumer concerns regarding personal information.

51. A survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do protect their privacy online.²⁰ As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.²¹

52. Thus, as consumer privacy concerns grow, consumers increasingly incorporate privacy concerns and values into their purchasing decisions, and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.²²

²⁰ See 2014 TRUSTe US Consumer Confidence Privacy Report, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

²¹ *Id.*

²² See Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), available at <https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html>.

53. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.²³

54. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.²⁴ As such, where a business offers customers a product or service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a product or service of less value than the product or service paid for.

III. Defendant Unlawfully Sells, Rents, Transmits, And Otherwise Discloses Its Customers' Personal Viewing Information

55. Defendant maintains vast digital databases comprised of its customers' Personal Viewing Information, including the names and addresses of

²³ See Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); see also European Network and Information Security Agency, *Study on Monetizing Privacy* (Feb. 27, 2012), available at <https://www.enisa.europa.eu/publications/monetising-privacy>.

²⁴ See Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available at <https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf>.

each customer and information reflecting the titles of specific videos and other audio-visual products that each of its customers has purchased.



56. During the time period relevant to this action, Defendant has monetized these databases by renting, selling, or otherwise disclosing their customers' Personal Viewing Information to data aggregators, data miners, data brokers, data appenders, and other third parties.

57. These factual allegations are corroborated by two pieces of publicly available evidence. For instance, as shown in the screenshot below, the Personal Viewing Information of 303,967 American consumers who purchased Defendant's video products, including healthcare nursing seminars, is offered for sale on the website of NextMark, Inc. ("NextMark") – one of many traffickers of this type of Personal Viewing Information – at a base price of "\$130.00/M [per thousand records]" (13.0 cents each):

HealthCare Nursing Seminar Attendees from PESI HealthCare Business Mailing List Mailing List

HealthCare Nursing Seminar Attendees from PESI HealthCare Business Mailing List is the leader of education within the healthcare community. Continuing Education Seminars, Conferences, On-Site Training and Webinars. PESI Healthcare Seminar Attendees: Current, Relevant, Effective.

[Get Count](#) [Get Pricing](#) [Get More Information](#)

SEGMENTS		COUNTS THROUGH 12/31/2023	MARKET:	BUSINESS
303,967 TOTAL UNIVERSE / BASE RATE		\$130.00/M	CHANNELS:	 
303,967 TOTAL UNIVERSE		\$130.00/M	SOURCE:	DIRECT RESPONSE
14,237 3 MONTH NURSING SEMINAR ATTENDEES		+ \$20.00/M	PRIVACY:	UNKNOWN
28,267 6 MONTH NURSING SEMINAR ATTENDEES		+ \$15.00/M	DMA?:	NO
51,545 12 MONTH NURSING SEMINAR ATTENDEES		+ \$10.00/M	STATUS:	STANDARD PROVIDER
FUNDRAISING		\$75.00/M	GEO:	USA
DESCRIPTION			GENDER:	87% FEMALE 8% MALE
HealthCare Nursing Seminar Attendees from PESI			SELECTS	
HealthCare provides current, relevant and effective on-site training programs for many enthusiastic medical professionals in all specialties. These individuals are eager to learn and grow within their healthcare practices and environments.			BUSINESS ADDRESS	\$15.00/M
			GENDER/SEX	\$15.00/M
			NO. OF EMPLOYEES	\$15.00/M
			ONE PER LOCATION	\$15.00/M
			SALES VOLUME	\$15.00/M
			SCF	\$10.00/M
			SEMINAR	\$20.00/M
			SEMINAR CATEGORY	\$20.00/M
			STATE	\$10.00/M
			TITLE	\$15.00/M
			ZIP	\$10.00/M
			ADDRESSING	
			KEY CODING	\$3.00/M
			DELIVERY FEE	\$75.00/F
			RELATED LISTS	
			<input type="checkbox"/> MEDICAL GROUP MANAGEMENT ASSOCIATION (MGMA)	
			<input type="checkbox"/> EMERGENCY NURSES ASSOCIATION (ENA)	
			<input type="checkbox"/> BOARD OF CERTIFICATION FOR EMERGENCY NURSING (BCEN)	
			<input type="checkbox"/> ASSOCIATION OF WOMEN'S HEALTH, OBSTETRIC AND NEONATAL NURSES (AWHONN)	
			<input type="checkbox"/> ONCOLOGY NURSING SOCIETY (ONS)	
			<input type="checkbox"/> MEDQOR - HEALTHCARE MASTERFILE	
			<input type="checkbox"/> ASSOCIATION OF AMERICAN MEDICAL COLLEGES (AAMC)	
			<input type="checkbox"/> NEW ENGLAND JOURNAL OF MEDICINE (NEJM)	
			<input type="checkbox"/> NATIONAL ASSOCIATION OF SOCIAL WORKERS (NASW) EMAIL AND MAILING LIST	
			<input type="checkbox"/> AMERICAN ACADEMY OF PHYSICIAN ASSISTANTS (AAPA)	
This list allows mailers and marketers to target accurately medical professionals looking to further their knowledge and practical experience in their respective fields.				
HealthCare Nursing Seminar Attendees from PESI HealthCare also purchase a wide range of educational products and reference materials such as books, audio tapes, home-study packages and videos.				
These are women and men who further their respective professions by way of distance training, online education, on-site training and by attending seminars.				
Through webinars and teleseminars, HealthCare Nursing Seminar Attendees from PESI HealthCare , utilize the latest communication tools to deliver an integrated learning experience that can be attended either at your desk or in a conference room. These types of events are a convenient way to receive focused education without traveling.				
Data Axle recommends the HealthCare Nursing Seminar Attendees from PESI HealthCare Business Mailing List for the following offers: Ad specialty catalogs, day planner/pen catalogs, small-business credit card offers, office furniture/supply catalogs, uniform apparel catalogs, hosiery / shoe catalogs, travel accessory catalogs, health publishing magazines, holiday card catalogs, food/gift offers, consumer gift offers, apparel catalogs, fundraising offers, consumer book offers and publications, news publications, health offers, medical supply catalogs, vitamin catalogs.				




See Exhibit A hereto.

58. Additionally, as shown in the screenshot below, the Personal Viewing Information of 199,167 American consumers who purchased Defendant’s video products, including mental health seminars, is offered for sale on the website of NextMark, Inc. (“NextMark”) – one of many traffickers of this type of Personal Viewing Information – at a base price of “\$130.00/M [per thousand records]” (13.0 cents each):

Mental Health Seminar Attendees from PESI Mailing List Mailing List

Mental Health Seminar Attendees from PESI represent a vast universe of professionals in many specialties dealing with therapy and counseling.

[Get Count](#) [Get Pricing](#) [Get More Information](#)

SEGMENTS	COUNTS THROUGH 12/31/2023	POPULARITY: ***** 99
199,167 TOTAL UNIVERSE / BASE RATE	\$130.00/M	MARKET: BUSINESS
199,167 TOTAL UNIVERSE	\$130.00/M	CHANNELS:  
12,957 3 MONTH SEMINAR ATTENDEES	+ \$20.00/M	SOURCE: DIRECT RESPONSE
35,468 6 MONTH SEMINAR ATTENDEES	+ \$15.00/M	PRIVACY: UNKNOWN
71,932 12 MONTH SEMINAR ATTENDEES	+ \$10.00/M	DMA?: NO
FUNDRAISING	\$75.00/M	STATUS: STANDARD PROVIDER
DESCRIPTION		GEO: USA
CMI Education Institute, Inc. is the non-profit parent company of PESI, MEDS-PDN, and CMI Education.		GENDER: 81% FEMALE 14% MALE
 <p>PESI is the largest behavioral health education company in the country, providing more than 4,000 seminars and conferences across the country each year. The trainings are designed by expert clinicians with the needs of professional adult learners in mind. Seminars for the mental health professionals provide practical, hands-on skills, strategies, techniques and interventions that improve the outcome of the people they serve. PESI has been connecting knowledge with need since 1979.</p> <p>The Mental Health Seminar Attendees from PESI Mailing List provides access to highly sought-after professionals, such as counselors, therapists, social workers, psychologists, nurses, teachers, marriage and family therapists, occupational therapists, physical therapists, speech language pathologists, and others in the helping professions.</p> <p>PESI provides mailers and marketers with leading behavioral health professionals who are looking to expand their awareness about treatments and therapy programs. These attendees purchase a wide range of educational products and reference materials including seminars, conferences, video webcasts, on-demand trainings, home study opportunities and books.</p> <p>Connect with individuals who share a strong commitment to improve their clients' quality of life as well as being up-to-date with the latest trends and techniques available in their respective fields.</p> <p>The Mental Health Seminar Attendees from PESI Mailing List are ideal for offers including: Ad specialty catalogs, day planner/pen catalogs, small-business credit card offers, office furniture/supply catalogs, uniform apparel catalogs, hosiery / shoe catalogs, travel accessory catalogs, health publishing magazines, holiday card catalogs, food/gift offers, consumer gift offers, apparel catalogs, fundraising offers, consumer book offers and publications, news publications, health offers, medical supply catalogs, vitamin catalogs.</p>		SELECTS
		COURSE HEADING \$15.00/M
		JOB TITLE \$15.00/M
		NO. OF EMPLOYEES \$15.00/M
		ONE PER LOCATION \$15.00/M
		SALES VOLUME \$15.00/M
		SCF \$10.00/M
		SIC/NAICS CODE \$15.00/M
		STATE \$10.00/M
		ZIP \$10.00/M
		ADDRESSING
		KEY CODING \$3.00/M
		DELIVERY FEE \$75.00/F
		RELATED LISTS
		NATIONAL ASSOCIATION OF SOCIAL WORKERS (NASW) EMAIL AND MAILING LIST
		AMERICAN MENTAL HEALTH COUNSELORS ASSOCIATION
		AMERICAN COUNSELING ASSOCIATION MEMBERS
		NATIONAL ASSOCIATION OF SCHOOL PSYCHOLOGISTS (NASP)
		AMERICAN ACADEMY OF CHILD & ADOLESCENT PSYCHIATRY (AACAP)
		AMERICAN ASSOCIATION FOR MARRIAGE & FAMILY THERAPY (AAMFT)
		JOURNAL WATCH PSYCHIATRY
		JACOB-CAMERON PUBLISHING
		COMPANY PSYCHOLOGY AND COUNSELING DATABASE
		AMERICAN BOARD OF CLINICAL SOCIAL WORK (ABCSW)
		COMPLETE MEDICAL'S ADDICTION COUNSELORS

See Exhibit B hereto.

59. Defendant’s “Healthcare Nursing Seminar Attendees” and “Mental Health Seminar Attendees” lists are offered for sale by NextMark, shown in the screenshots above, collectively contain Personal Viewing Information for each of the 503,134 American consumers whose information appears on the lists, including each person’s name, postal address, e-mail address, gender, age, and income, as well as the prerecorded particular audio-visual product(s) they purchased from Defendant (i.e., the titles of the prerecorded videos purchased) and the amount of money they spent on those purchases.

60. As a result of Defendant’s data compiling and sharing practices, companies have obtained and continue to obtain the Personal Viewing Information of Defendant’s customers, together with additional sensitive personal information that has been appended thereto by data appenders and others.

61. Plaintiff is informed and believes, and thereupon alleges, that numerous of the third parties to whom Defendant has transmitted and/or otherwise disclosed their customers’ Personal Viewing Information, either directly or indirectly through an intermediary or intermediaries, have in turn sold, rented, transmitted, or otherwise disclosed that Personal Viewing Information (together with other sensitive personal demographic and lifestyle information appended thereto by data appenders and other entities) to other third parties, including other data brokers, data miners, data appenders, and marketing companies.

62. Defendant's disclosure of Personal Viewing Information has put its customers at risk of serious harm from scammers. For example, as a result of Defendant's disclosure of Personal Viewing Information, any person or entity could obtain a list with the names and addresses of all women residing in Connecticut who purchased prerecorded healthcare nursing seminars related to children's healthcare from Defendant during the past 12 months. Such a list is available for sale for approximately \$180.00 per thousand customers listed.

63. Additionally, any person or entity could obtain a list with the names and addresses of persons residing in Connecticut who purchased prerecorded mental health seminars related to children's mental health from Defendant during the past 12 months. Such a list is available for sale for approximately \$155.00 per thousand customers listed.

64. Defendant did not seek Plaintiff or any other customers' prior written consent to the disclosure of their Personal Viewing Information (in writing or otherwise) and their customers remain unaware that their Personal Viewing Information and other sensitive data is being sold, rented and exchanged on the open market.

IV. Defendant Uses the Meta Pixel to Systematically Disclose its Customers' Personal Viewing Information to Meta

65. As alleged below and in addition to Defendant's independent practice of transmitting Plaintiff and the Class members' Personal Viewing Information to data brokers and data appenders, when a consumer purchases a specific prerecorded video product from Defendant's website, the Meta Pixel technology that Defendant intentionally installed on its website transmits the fact that a consumer purchased prerecorded video materials alongside his or her FID to Meta, without the purchaser's consent and in clear violation of the VPPA.

A. The Meta Pixel

66. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta".²⁵ Meta is now the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

67. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to monitor and track the actions taken by visitors to their websites and to report them back to Meta.

²⁵ See Facebook, "Company Info," available at <https://about.fb.com/company-info/>.

This allows companies like Defendant to build detailed profiles about their customers and to serve them with highly targeted advertising.

68. Additionally, a Meta Pixel installed on a company's website allows Meta to "match [] website visitors to their respective Facebook User accounts."²⁶ This is because Meta has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name²⁷ – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

69. The Meta Pixel allows online-based companies like Defendant to build detailed profiles about their visitors by collecting information about how they interact with their websites, and to then use the collected information to service highly targeted advertising to them.

²⁶ Meta, "Get Started – Meta Pixel," available at <https://developers.facebook.com/docs/meta-pixel/get-started/>.

²⁷ For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

70. Additionally, a Meta Pixel installed on a company's website allows Meta "to match . . . website visitors to their respective [Meta] User accounts."²⁸ Meta is able to do this because it has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name²⁹ – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor.

71. The FID is stored in a small piece of code known as a "cookie" that Meta launches and stores in the internet browsers of each Meta accountholder's device(s) to distinguish between website visitors.³⁰

72. As Meta's developer's guide explains, installing the Meta Pixel on a website allows Meta to track actions that users with Meta accounts take on the site. Meta states that "Examples of [these] actions include adding an item to their shopping cart or making a purchase."³¹

²⁸ Meta, *Get Started—Meta Pixel*, <https://developers.facebook.com/docs/meta-pixel/get-started/>

²⁹ For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

³⁰ Meta, *How to Create a Custom Audience from Your Customer List*, <https://www.facebook.com/business/help/471978536642445?id=1205376682832142> (last visited Nov. 11, 2024).

³¹ Meta, *About Meta Pixel*, available at <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

73. The default configuration of the Meta Pixel, which is what Defendant used, enables website visitor tracking because the Meta Pixel automatically detects first-party cookie data from the particular website that the visitor is on and then automatically matches it with third-party cookie data from Meta such as the c_user cookie that houses a person's FID.³²

74. Meta's Business Tools Terms govern the use of Meta's Business Tools, including the Meta Pixel.³³

75. Meta's Business Tools Terms state that website operators may use Meta's Business Tools, including the Meta Pixel, to transmit the "Contact Information" and "Event Data" of their website visitors to Meta.

76. Meta's Business Tools Terms define "Contact Information" as "information that personally identifies individuals, such as names, email addresses, and phone numbers"³⁴

77. Meta's Business Tools Terms state: "You instruct us to process the Contact Information solely to match the Contact Information against user IDs [e.g.,

³² Meta, *Business Help Center: About cookie settings for the Meta Pixel*, FACEBOOK, <https://www.facebook.com/business/help/471978536642445?id=1205376682832142> (last visited Nov. 11, 2024).

³³ Meta, *Meta Business Tools Terms*, available at https://www.facebook.com/legal/technology_terms.

³⁴ *Id.*

FIDs] (“Matched User IDs”), as well as to combine those user IDs with corresponding Event Data.”³⁵

78. The Business Tools Terms define “Event Data” as, *inter alia*, “information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products.”³⁶

79. Website operators use the Meta Pixel to send information about visitors to their websites to Meta. Every transmission to Meta accomplished through the Meta Pixel includes at least two elements: (1) the website visitor’s FID and (2) the webpage’s URL triggering the transmission.

80. Depending on the configuration of the Meta Pixel, the website may also send Event Data to Meta. Defendant has configured the Meta Pixel on its websites to send Event Data to Meta, including the page view and purchase events.

81. When website operators make transmissions to Meta through the Meta Pixel, none of the following categories of information are hashed or encrypted: the visitor’s FID, the website URL, or the Event Data.

³⁵ *Id.*

³⁶ *Id.*

82. Every website operator installing the Meta Pixel must agree to the Meta Business Tools Terms.³⁷

83. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after clearing browser history.

84. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

85. Simply put, if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are then able to “track [] the people and type of actions they take,”³⁸ including, as relevant here, the specific prerecorded video material that they purchase on the website.

³⁷ *See id.*

³⁸ Meta, “Retargeting: How to Advertise to Existing Customers with Ads on Facebook,” available at https://www.facebook.com/business/goals/retargeting?checkpoint_src=any.

A. Defendant Knowingly Uses the Meta Pixel to Transmit the Personal Viewing Information of its Customers to Meta

86. Defendant sells a wide variety of prerecorded video materials, including conferences, seminars, workshops, online/on-demand courses, CDs and DVDs on its main website, www.pesi.com, and its network of affiliate websites, which include websites such as <https://www.psychotherapynetworker.org/>, and others.

87. To purchase prerecorded video material from Defendant's Website, a person must provide at least his or her name, email address, billing address, and credit or debit card (or other form of payment) information.

88. During the purchase process on Defendant's website, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the person who made the purchase and the specific title of video material that the person purchased (as well as the URL where such video material is available for purchase).

89. In order to take advantage of the targeted advertising and other informational and analytical services offered by Meta, Defendant intentionally programmed its website and its affiliates' websites (by following step-by-step instructions from Meta's website) to include the Meta Pixel code, which systematically transmits to Meta the FID of each person with a Meta account who

purchases prerecorded video material on one of Defendant's websites, along with the specific title of the prerecorded video material that the person purchased.

90. With only a person's FID and the title of the prerecorded video material (or URL where such material is available for purchase) that the person purchased from Defendant on of its websites—all of which Defendant knowingly and systematically provides to Meta—any ordinary person could learn the identity of the person to whom the FID corresponds and the title of the specific prerecorded video material that the person purchased (and thus requested and obtained). This can be accomplished simply by accessing the URL www.facebook.com/ and inserting the person's FID.

91. Defendant's practice of disclosing the Personal Viewing Information of its customers to Meta continued unabated for the duration of the two-year period preceding the filing of this action. At all times relevant hereto, whenever Plaintiff or any other person purchased prerecorded video material from Defendant on any of its websites, Defendant disclosed to Meta (*inter alia*) the specific title of the video material that was purchased (including the URL where such material is available for purchase), along with the FID of the person who purchased it (which, as discussed above, uniquely identified the person).

92. At all times relevant hereto, Defendant knew the Meta Pixel was disclosing its customers' Personal Viewing Information to Meta.

93. Although Defendant could easily have programmed its website so that none of its customers' Personal Viewing Information is disclosed to Meta, Defendant instead chose to program its website so that all of its customers' Personal Viewing Information is disclosed to Meta.

94. Before transmitting its customers' Personal Viewing Information to Meta, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

95. By intentionally disclosing to Meta Plaintiff's and its other customers' FIDs together with the specific video material that they each purchased, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

V. Defendant Uses the Other Tracking Technologies to Systematically Disclose its Customers' Personal Viewing Information to Third Parties

96. As alleged below and in addition to Defendant's independent practice of transmitting Plaintiff and the Class members' Personal Viewing Information to data brokers and data appenders, when a consumer purchases a specific prerecorded video product from Defendant's website, the Google and Pinterest technology that Defendant intentionally installed on its website transmit the fact that a consumer purchased prerecorded video materials alongside unique identifiers that identify the purchaser, without the purchaser's consent and in clear violation of the VPPA.

A. Google

97. Defendant intentionally installed Google Analytics, Google AdSense, and Google Leads extension on its website, which operates in a similar fashion to the Meta Pixel. Specifically, when a person purchases a prerecorded video from Defendant's website, Defendant discloses to Google Analytics, through the operation of the Google Analytics, the user's (i) hashed email address, (ii) Google Analytics client ID, (iii) the title, unique numerical identifier, and URL of the video the user is watching, and (iv) excessive amounts of uniquely identifiable data points, or predefined user dimensions, just short of a person's name that include: age, browser type, city, continent and subcontinent, country, device brand, gender, interests, language, operating system, OS version, IP address, platform, region.³⁹

98. When a subscriber to Defendant's website requests or obtains a particular prerecorded video by clicking on it, the title of the prerecorded video content and the prerecorded video content's product number are transmitted to Google Analytics alongside the subscriber's client id ("cid"),⁴⁰ hashed email

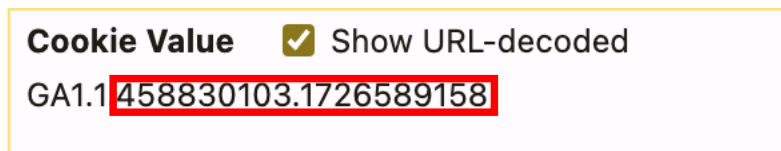
³⁹ Google Analytics Help, *Dimensions and metrics [GA4] Predefined user dimensions signals*, https://support.google.com/analytics/answer/9268042?visit_id=638630753515343005-1876215053&rd=2 (last visited Sept. 28, 2024).

⁴⁰ Google Analytics Help, *[GA4] Data collection*, <https://support.google.com/analytics/answer/11593727?hl=en> (last visited Sept. 28, 2024) ("Google Analytics stores a client ID in a first-party cookie named _ga to distinguish unique users and their sessions on your website.").

address, NID,⁴¹ IP address, and unique device identifiers. This information can be used by an ordinary person to identify the specific subscriber.

99. Specifically, each subscriber to Defendant’s website is assigned a “cid” by Defendant and its use of Google technology to distinguish between individual users and their sessions on Defendant’s website.

100. A subscriber’s cid and unique id “uid” are also communicated through cookies within that same Google Analytics code. The cookie values are displayed in the developer settings of the browser and reveal the particular cid within the `_ga` cookie, as seen in the following exemplar:



101. This `_ga` cookie is comprised of four parts separated by periods: (1) a version number “GA[#]”, (2) the number of components at the domain, (3) a unique ID # for the user, and (4) a timestamp of the user’s first visit to the site. The last two parts collectively make up the client id.

⁴¹ Defendant even discloses a unique identifier to Google Analytics for each subscriber who is not signed into their Google account at the time they request or obtain videos from Defendant’s website, and that identifier is the NID which directly relates back to one’s Google account. See Google, *How Google uses cookies*, <https://policies.google.com/technologies/cookies> (last visited Sept. 28, 2024) (“The ‘NID’ cookie is used to show Google ads in Google services for *signed-out users*”) (emphasis added).

102. An email address is a personally identifying string of characters that designate an electronic mailbox. Any ordinary person can use an e-mail address to uniquely identify the individual to whom it belongs. Voluminous services exist which enable individuals to look up the owners of a particular email address.

103. A “hash” is an algorithm used to create a digital summary, or fingerprint, of the input. However, the Federal Trade Commission has warned companies for over a decade that hashing is an insufficient method of anonymizing information, including as recently as July 24, 2024.⁴² Thus, even in hashed form, email addresses are traceable to individuals.

104. The IP addresses transmitted by Defendant to Google Analytics create an approximate map to follow the subscriber across devices and locations. This is because the IP address changes depending on the subscriber’s location and device. In the case of Plaintiff, each time they viewed a particular video from Defendant’s website, Defendant disclosed their personal IP addresses corresponding to the mobile device or computer used. If Plaintiff used a different device from a different location, Google Analytics received a different IP address, and each IP address

⁴² Ed Felten, *Does Hashing Make Data “Anonymous”?*, Federal Trade Commission (Apr. 22, 2012), available at <https://www.ftc.gov/policy/advocacy-research/tech-atftc/2012/04/does-hashing-make-data-anonymous>; Federal Trade Commission, *No, Hashing Still Doesn’t Making Your Data Anonymous* (July 24, 2024), available at <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous>.

remained associated with the individual Plaintiff's pesi.com account, client ID, hashed email address, and other unique device identifiers disclosed to Google Analytics.

105. In sum, as an example of the information disclosed by Defendant to Google Analytics, the information would reveal that a 34-year-old woman from Charlotte, North Carolina (North America - USA) at her home's IP Address 69.217.130.96 using Mozilla Firefox on a MacOSX Sierra Studio computer requested or obtained a specific video product from www.pesi.com.

106. While the information already disclosed by Defendant to Google Analytics is sufficient for identification of a particular user, the unique identifiers are also being told to Google AdSense and Google Leads Extension, which are not bound by the anonymized data collection of Google Analytics. Therefore, upon information and belief, Google AdSense and Google Leads are automatically able to amalgamate the information disclosed with data already existing within Google's servers to specifically identify a user back to their corresponding Gmail account to better serve that user with advertising.

107. Simply put, when a person requests or obtains a prerecorded video from Defendant's website, Google Analytics or any ordinary person can identify that user by email address, client ID, or by using the approximate map of IP addresses when coupled with the other identifiers discussed above. Separately,

Google AdSense and Leads can identify a user if it chooses through the automatic culling together of preexisting data within its servers including that person's gmail account.

B. Pinterest

108. Defendant intentionally installed the Pinterest Tag on its website, which operates in a similar fashion to the Meta Pixel. Specifically, Pinterest assigns each accountholder with a user ID ("uid"), which is found in the "s_a" cookie that is an encrypted value identifying only one particular person's Pinterest account as they navigate non-Pinterest websites, similar to Meta's FID. To create a Pinterest account, a person must provide their first and last name, age, gender (optional), email address, country, region, and preferred language. This information is directly linked to a person's s_a encrypted value, thereby directly allowing for identification of one particular person per s_a cookie.

109. The same s_a value is communicated to Defendant via the Pinterest Tag and Defendant then stores the same value in their own cookie. Defendant would not know anything about a particular Pinterest user but for its installation of the Pinterest Tag on its website.

110. Simply put, when a person requests or obtains a prerecorded video from Defendant's website, Pinterest or any ordinary person can identify that user by uid in the s_a cookie or other information disclosed via the Pinterest Tag by simply

going to a person's Pinterest profile and right-clicking "Inspect Source" and cross referencing the information disclosed against the information in the source.

111. At all times relevant hereto, Defendant knew that Google Analytics and Pinterest Tag were disclosing its customers' Personal Viewing Information to Google and Pinterest.

112. Before transmitting its customers' Personal Viewing Information to Google and Pinterest, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

113. By intentionally disclosing to Google and Pinterest Plaintiff's and its other customers' unique identifiers together with the specific video material that they each purchased, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

114. Plaintiff seeks to represent four classes defined as follows:

Data Brokerage Class: All persons in the United States who, during the two years preceding the filing of this action, purchased prerecorded video material from Defendant and had their Personal Viewing Information disclosed to a third-party by Defendant's rental, sale, or other disclosure by way of Nextmark lists.

Meta Pixel Class: All persons in the United States who, during the two years preceding the filing of this action, purchased prerecorded video material or services from Defendant's www.pesi.com Website or any of its affiliates' websites while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

Google Analytics Class: All persons in the United States who, during the two years preceding the filing of this action, purchased prerecorded video material or services from Defendant's www.pesi.com Website or any of its affiliates' websites while maintaining an account with Alphabet, Inc. f/k/a Google.

Pinterest Tag Class: All persons in the United States who, during the two years preceding the filing of this action, purchased prerecorded video material or services from Defendant's www.pesi.com Website or any of its affiliates' websites while maintaining an account with Pinterest, Inc.

115. Members of each Class are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Classes number in at least the tens of thousands. The precise number of members in each Class and their identities are unknown to Plaintiff at this time but may be determined through discovery. Members of each Class may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

116. Common questions of law and fact exist for all Classes and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to (a) whether Defendant embedded the Meta Pixel, Google Analytics, and Pinterest Tag on its Website that monitors and tracks actions taken by visitors to its Website; (b) whether Defendant reports the actions and information of visitors to Meta, Google, and Pinterest; (c) whether Defendant knowingly disclosed Plaintiff's and Class members' Personal Viewing Information to Meta, Google, and Pinterest; (d) whether Defendant's conduct

violates the Video Privacy Protection Act, 18 U.S.C. § 2710; and (e) whether Plaintiff and the Classes are entitled to a statutory damage award of \$2,500, as provided by the VPPA.

117. The named Plaintiff's claims are typical of the claims of the Classes in that the Defendant's conduct toward the putative class is the same. That is, Defendant embedded the Tracking Technologies on its Website to monitor and track actions taken by consumers on its Website and report this to Meta, Google, and Pinterest. Further, the named Plaintiff and members of the Classes suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Private Purchase Information to Meta, Google, and Pinterest.

118. Plaintiff is an adequate representative of the Classes because she is interested in the litigation; her interests do not conflict with those of the Classes she seeks to represent; she has retained competent counsel experienced in prosecuting class actions; and she intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of all members of each Class.

119. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class member

may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication of the common questions of law and fact, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSES OF ACTION

I. Count 1: Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710 (Data Brokerage Class)

120. Plaintiff repeats the allegations asserted in paragraphs 1-64 and 114-119 as if fully set forth herein.

121. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

122. As defined in 18 U.S.C. § 2710(a)(4), a “video tape service provider” is “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]” Defendant is a “video tape service provider” as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

123. As defined in 18 U.S.C. § 2710(a)(1), a “‘consumer’ means any renter, purchaser, or consumer of goods or services from a video tape service provider.” As alleged above, Plaintiff and Data Brokerage Class members are each a “consumer” within the meaning of the VPPA because they each purchased a subscription to access prerecorded video material or services from Defendant’s Website that was sold and delivered to them by Defendant.

124. As defined in 18 U.S.C. § 2710(a)(3), “‘personally identifiable information’ includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” The Personal Viewing Information that Defendant rented, sold, or otherwise disclosed to data aggregators, data brokers, data appenders, and the like constitutes “personally identifiable information” as defined in 18 U.S.C. § 2710(a)(3) because it identified Plaintiff and Data Brokerage Class members to third parties as an

individual who purchased, and thus “requested or obtained,” prerecorded video content from Defendant’s Website.

125. Defendant knowingly disclosed Plaintiff’s and Class members’ Personal Viewing Information to data aggregators, data brokers, data appenders because Defendant knowingly rented, sold, or otherwise disclosed their customers’ Personal Viewing Information to data aggregators, data miners, data brokers, data appenders, and other third parties.

126. Defendant failed to obtain informed written consent from Plaintiff or Class members authorizing it to disclose their Personal Viewing Information to data aggregators, data brokers, data appenders, or any other third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who purchased prerecorded video material or services on its Website (including Plaintiff or Data Brokerage Class members) informed, written consent that was given in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis

or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

127. By disclosing Plaintiff's and Data Brokerage Class members' Personal Viewing Information, Defendant violated their statutorily protected right to privacy in their Personal Viewing Information.

128. Consequently, Defendant is liable to Plaintiff and Data Brokerage Class members for damages in the statutorily set sum of \$2,500. 18 U.S.C. § 2710(c)(2)(A).

II. Count 2: Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710 (Meta Pixel Class)

129. Plaintiff repeats the allegations asserted in paragraphs 1-55, 65-95, and 114-119 as if fully set forth herein.

130. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

131. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape service provider" as defined in

18 U.S.C. § 2710(a)(4) because it is engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

132. As defined in 18 U.S.C. § 2710(a)(1), a “‘consumer’ means any renter, purchaser, or consumer of goods or services from a video tape service provider.” As alleged above, Plaintiff and Meta Pixel Class members are each a “consumer” within the meaning of the VPPA because they each purchased prerecorded video material or services from Defendant’s Website that were sold and delivered to them by Defendant.

133. As defined in 18 U.S.C. § 2710(a)(3), “‘personally identifiable information’ includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” The Personal Viewing Information that Defendant transmitted to Meta constitutes “personally identifiable information” as defined in 18 U.S.C. § 2710(a)(3) because it identified Plaintiff and Meta Pixel Class members to Meta as an individual who purchased, and thus “requested or obtained,” prerecorded video content from Defendant’s Website.

134. Defendant knowingly disclosed Plaintiff’s and Meta Pixel Class members’ Personal Viewing Information to Meta via the Meta Pixel technology because Defendant intentionally installed and programmed the Meta Pixel code on

its Website, knowing that such code would transmit the prerecorded video content purchased by its consumers and the purchasers' unique identifiers (including FIDs).

135. Defendant failed to obtain informed written consent from Plaintiff or Meta Pixel Class members authorizing it to disclose their Personal Viewing Information to Meta or any other third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who purchased prerecorded video material or services on its Website (including Plaintiff or Meta Pixel Class members) informed, written consent that was given in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

136. By disclosing Plaintiff's and Meta Pixel Class members' Personal Viewing Information, Defendant violated their statutorily protected right to privacy in their Personal Viewing Information.

137. Consequently, Defendant is liable to Plaintiff and Meta Pixel Class members for damages in the statutorily set sum of \$2,500. 18 U.S.C. § 2710(c)(2)(A).

III. Count 3: Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710 (Google Analytics Class)

138. Plaintiff repeats the allegations asserted in paragraphs 1-55, 96-107, and 111-119, as if fully set forth herein.

139. The VPPA prohibits a “video tape service provider” from knowingly disclosing “personally identifying information” concerning any “consumer” to a third party without the “informed, written consent (including through an electronic means using the Internet) of the consumer.” 18 U.S.C. § 2710.

140. As defined in 18 U.S.C. § 2710(a)(4), a “video tape service provider” is “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]” Defendant is a “video tape service provider” as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

141. As defined in 18 U.S.C. § 2710(a)(1), a “‘consumer’ means any renter, purchaser, or consumer of goods or services from a video tape service provider.” As

alleged above, Plaintiff and Google Analytics Class members are each a “consumer” within the meaning of the VPPA because they each purchased prerecorded video material or services from Defendant’s Website that were sold and delivered to them by Defendant.

142. As defined in 18 U.S.C. § 2710(a)(3), “‘personally identifiable information’ includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” The Personal Viewing Information that Defendant transmitted to Google constitutes “personally identifiable information” as defined in 18 U.S.C. § 2710(a)(3) because it identified Plaintiff and Google Analytics Class members to Google as an individual who purchased, and thus “requested or obtained,” prerecorded video content from Defendant’s Website.

143. Defendant knowingly disclosed Plaintiff’s and Google Analytics Class members’ Personal Viewing Information to Google via the Google Analytics’s integrated technology because Defendant intentionally installed and programmed Google Analytics on its Website, knowing that such code would transmit the prerecorded video content purchased by its consumers and the purchasers’ unique

identifiers (including cid, uid, hashed email address, IP addresses,⁴³ and other user identifiers).

144. Defendant failed to obtain informed written consent from Plaintiff or Google Analytics Class members authorizing it to disclose their Personal Viewing Information to Google or any other third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who purchased prerecorded video material or services on its Website (including Plaintiff or Google Analytics Class members) informed, written consent that was given in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

145. By disclosing Plaintiff's and Google Analytics Class members' Personal Viewing Information, Defendant violated their statutorily protected right to privacy in their Personal Viewing Information.

⁴³ IP addresses are the locating identification for computers or devices that connect to the Internet or other Transfer Control Protocol / Internet Protocol ("TCP/IP") network.

146. Consequently, Defendant is liable to Plaintiff and Google Analytics Class members for damages in the statutorily set sum of \$2,500. 18 U.S.C. § 2710(c)(2)(A).

IV. Count 4: Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710 (Pinterest Tag Class)

147. Plaintiff repeats the allegations asserted in paragraphs 1-55 and 96, 108-119 as if fully set forth herein.

148. The VPPA prohibits a “video tape service provider” from knowingly disclosing “personally identifying information” concerning any “consumer” to a third party without the “informed, written consent (including through an electronic means using the Internet) of the consumer.” 18 U.S.C. § 2710.

149. As defined in 18 U.S.C. § 2710(a)(4), a “video tape service provider” is “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]” Defendant is a “video tape service provider” as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

150. As defined in 18 U.S.C. § 2710(a)(1), a “‘consumer’ means any renter, purchaser, or consumer of goods or services from a video tape service provider.” As

alleged above, Plaintiff and Pinterest Tag Class members are each a “consumer” within the meaning of the VPPA because they each purchased prerecorded video material or services from Defendant’s Website that were sold and delivered to them by Defendant.

151. As defined in 18 U.S.C. § 2710(a)(3), “‘personally identifiable information’ includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” The Personal Viewing Information that Defendant transmitted to Pinterest constitutes “personally identifiable information” as defined in 18 U.S.C. § 2710(a)(3) because it identified Plaintiff and Pinterest Tag Class members to Pinterest as an individual who purchased, and thus “requested or obtained,” prerecorded video content from Defendant’s Website.

152. Defendant knowingly disclosed Plaintiff’s and Pinterest Tag Class members’ Personal Viewing Information to Pinterest via the Pinterest Tag technology because Defendant intentionally installed and programmed the Pinterest Tag code on its Website, knowing that such code would transmit the prerecorded video content purchased by its consumers and the purchasers’ unique identifiers (including the s_a cookie, uid, and other user and device identifiers identified above).

153. Defendant failed to obtain informed written consent from Plaintiff or Pinterest Tag Class members authorizing it to disclose their Personal Viewing

Information to Pinterest or any other third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who purchased prerecorded video material or services on its Website (including Plaintiff or Pinterest Tag Class members) informed, written consent that was given in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

154. By disclosing Plaintiff's and Pinterest Tag Class members' Personal Viewing Information, Defendant violated their statutorily protected right to privacy in their Personal Viewing Information.

155. Consequently, Defendant is liable to Plaintiff and Pinterest Tag Class members for damages in the statutorily set sum of \$2,500. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendant PESI, Inc. as follows:

- a) For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Classes and Plaintiff's attorneys as Class Counsel to represent the Classes;
- b) For an order declaring that Defendant's conduct as described herein violated the VPPA;
- c) For an order finding in favor of Plaintiff and the Classes and against Defendant on all counts asserted herein;
- d) For an award of \$2,500.00 to Plaintiff and members of the Classes, as provided by 18 U.S.C. § 2710(c);
- e) For an order permanently enjoining Defendant from disclosing the Personal Viewing Information of its customers to third parties in violation of the VPPA;
- f) For prejudgment interest on all amounts awarded; and
- g) For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiff and the Classes under Rule 23 and 18 U.S.C. § 2710(c).

Respectfully submitted,

Dated: December 6, 2024

HEDIN LLP

/s/ Frank S. Hedin

Frank S. Hedin

HEDIN LLP

1395 Brickell Ave., Suite 610

Miami, Florida 33131-3302

Telephone: (305) 357-2107

Facsimile: (305) 200-8801

fhedin@hedinllp.com

Elliot O. Jackson

HEDIN LLP

1395 Brickell Ave., Suite 610

Miami, Florida 33131-3302

Telephone: (305) 357-2107

Facsimile: (305) 200-8801

Ejackson@hedinllp.com

*Counsel for Plaintiff and Putative
Classes*